Política de Segurança Cibernética

1. Introdução

Nossa prioridade é garantir uma experiência simples e segura para você. Pensando nisso, construímos uma política com práticas que consideram o ambiente de segurança da informação atual e futuro.

Os padrões foram baseados na ABNT NBR ISO/IEC 27001, nas regulamentações, legislação e contratos vigentes. Valorizamos nossos clientes e entendemos o quanto a segurança cibernética é importante para usufruírem dos nossos serviços com tranquilidade.

A segurança das suas informações está no nosso DNA e disponibilizamos aqui um resumo da nossa Política de Segurança Cibernética para que você possa conhecer um pouco mais das nossas diretrizes para proteção dos seus dados.

2. Objetivo

Manter a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob a guarda da Clicksign. Estabelecer medidas para a proteção da infraestrutura que suporta os serviços e atividades de negócio. Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

3. Público Alvo

Empresas parceiras e fornecedores que tenham acesso e/ou utilizem, direta ou indiretamente, informações e ativos internos para prestação de serviços à Clicksign.

Todos os colaboradores da Clicksign e fornecedores que tenham acesso ou utilizem, direta ou indiretamente, suas informações e ativos internos para prestação de serviços.

4. Termos e Definições

| Confidencialidade

Garantir que as informações são disponibilizadas ou divulgadas apenas a indivíduos, entidades ou processos autorizados.

| Integridade

Garantir que as informações são precisas, completas e protegidas de alterações indevidas, intencionais ou acidentais.

| Disponibilidade

Garantir que as informações são acessíveis e utilizáveis sob demanda por indivíduos, entidades ou processos autorizados.

5. Diretrizes Gerais

5.1. Gestão de Acesso

O acesso a sistemas, recursos e outros ativos de informação deve ser concedido mediante a uma autenticação válida e baseado em:

- Necessidade de negócio;
- O princípio do menor privilégio;
- Segregação de funções.

Os acessos devem ser gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação.

A composição das senhas devem seguir os requisitos de complexidade e ser únicas. Não devem ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar.

Ativos de informação considerados críticos, que armazenem e/ou processem informações sensíveis, devem ser restringidos às áreas segregadas da rede, com controle de acesso apropriado.

5.2. Auditoria

Logs e trilhas de auditoria devem ser habilitados em ambientes de produção, protegidos de acessos e alterações não autorizados e registrar:

- Que atividade foi executada;
- Quem executou a atividade;
- Quando a atividade foi executada;
- Onde a atividade foi executada.

5.3. Criptografia

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade,

autenticidade e/ou a integridade da informação.

Algoritmos criptográficos devem ser aplicados conforme a necessidade em dados em repouso, em trânsito e/ou em uso.

6. Monitoramento

Ferramentas e processos para monitorar e impedir que informações sensíveis deixem o ambiente interno de uma organização sem autorização devem estar implementados.

Soluções e/ou processos que permitam a prevenção, detecção, e identificação de ataques a componentes da infraestrutura da Clicksign devem estar implementados.

A utilização dos recursos deve ser monitorada e ajustada e as projeções serem feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

7. Vulnerabilidades

Um processo de gerenciamento do ciclo de vida de vulnerabilidades, desde a identificação até a remediação, incluindo diretrizes para documentação, emissão de relatórios e divulgação deve estar implementado.

Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam

obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.

8. Código Malicioso

Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

Soluções de software anti-malware de detecção, prevenção e recuperação ou controles equivalentes devem estar implementadas para proteger o ambiente da Clicksign.

9. Backup

Cópias de segurança das informações, softwares e das imagens do sistema, devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

10. Desenvolvimento de Software

Durante o ciclo de vida de desenvolvimento de software, requisitos de segurança devem ser aplicados para garantir a confidencialidade, integridade e disponibilidade das informações.

Deve ser feita uma avaliação de segurança antes da implementação de qualquer nova tecnologia, ferramenta ou solução em produção.

11. Incidente de Segurança Cibernética

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

O consumo e compartilhamento de informações de incidentes e ameaças com outras instituições locais e globais deve ser feito por canais seguros.

12. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios (PCN) visa garantir que, em situação de crise, os processos essenciais e críticos sejam devidamente mantidos, preservando assim a continuidade de funções de negócios, operações e serviços críticos.

13. Treinamento e Conscientização

Treinamentos de conscientização devem ser obrigatórios e realizados anualmente, apresentando os princípios de segurança da informação para auxiliar os funcionários a reconhecer situações de risco e agir corretamente.

14. Análise crítica das políticas para segurança da informação

As políticas para a segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

15. Avaliação de Fornecedores

Avaliações de fornecedores devem ser estabelecidas e documentadas para assegurar que não existem desentendimentos entre a Clicksign e o fornecedor, com relação à obrigação de ambas as partes com o cumprimento dos requisitos de segurança da informação relevantes.

16. Atualizações

A Política de Segurança Cibernética e demais políticas devem ser revisadas, no mínimo, a cada dois anos.

17. Comunicação

Em caso de dúvida, questão ou preocupação em relação a esta Política, entre em contato através de segurança@clicksign.com.